

MATH 567 FALL 2008, NUMBER THEORY I, SOLUTIONS 4

1. Show that if $f(x)$ is a polynomial with integer coefficients and if $f(a) \equiv k \pmod{m}$, then $f(a + tm) \equiv k \pmod{m}$ for every integer t . Write $f(x) = \sum_{j=0}^d a_j x^j$ with $a_j \in \mathbb{Z}$. We have $(a + tm)^j = \sum_{h=0}^j \binom{j}{h} a^h (tm)^{j-h} \equiv a^j \pmod{m}$. Thus $f(a + tm) \equiv \sum_{j=0}^d a_j a^j = f(a) \pmod{m}$.

2. Prove that any fourth power must have one of 0, 1, 5, 6 for its unit digit. Since $(-n)^4 \equiv n^4 \pmod{10}$ it suffices to consider $0^4 = 0$, $1^4 = 1$, $2^4 = 16$, $3^4 = 81$, $4^4 = 256$, $5^4 = 625$.

3. Show that $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$. By Wilson's theorem $70! \equiv -1 \pmod{71}$. Also $64.65 \dots 70 \equiv -7.6.5.4.3.2 \equiv -7.5.2.72 \equiv -70 \equiv 1 \pmod{71}$.

4. Prove that for any integer n , (i) $n^7 - n$ is divisible by 42, (ii) $n^{13} - n$ is divisible by 2730. (i) By Fermat's little theorem, $n^7 \equiv n \pmod{7}$, and $n^7 \equiv (n^3)2.n \equiv n^3 \equiv n \pmod{3}$, and trivially $n^7 \equiv n \pmod{2}$. Thus $42|n^7 - n$. (ii) Again by repeated use of Fermat, $n^{13} \equiv n \pmod{13}$, $n^{13} \equiv n^7.n^6 \equiv n.n^6 \equiv n \pmod{7}$, $n^{13} \equiv (n^5)^2.n^3 \equiv n^2.n^3 \equiv n \pmod{5}$, $n^{13} \equiv (n^3)^4.n \equiv n^4.n \equiv n^3.n^2 \equiv n^3 \equiv n \pmod{3}$, and finally trivially $n^{13} \equiv n \pmod{2}$.

5. Prove that if $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$. By Fermat, $a \equiv a^p \equiv b^p \equiv b \pmod{p}$. Hence $a = b + hp$ for some integer h . Hence $a^p - b^p = \sum_{j=1}^p \binom{p}{j} (mp)^j b^{p-j}$, and $p^2 | \binom{p}{j} p^j$ when $1 \leq j \leq p$.

6. Prove that if m is an odd positive integer, then the sum of any complete set of residues modulo m is $0 \pmod{m}$. If m is any integer with $m > 2$, then prove the analogous result for any reduced system of residues modulo m . We have $r + (m - r) \equiv 0 \pmod{p}$ and in either case there are no residues r with $1 \leq r \leq m - 1$ and $r \equiv m - r \pmod{m}$. Moreover, $(r, m) = 1$ iff $(m - r, m) = 1$. Hence in either case the residues with $1 \leq r \leq m - 1$ can be paired off so that their sum is $0 \pmod{m}$.

7. The numbers $F_n = 2^{2^n} + 1$ are called Fermat numbers. F_0 through F_4 are prime. Fermat had conjectured that F_n is always prime. Show that $641|F_5$. Suppose that p is a prime with $p|F_n$. Let e denote the smallest positive integer such that $2^e \equiv 1 \pmod{p}$. (i) Show that e exists and $e|2^{n+1}$. (ii) Show that $e \nmid 2^n$. (iii) Show that $p \equiv 1 \pmod{2^{n+1}}$. $2^{32} + 1 = (2^{16})^2 + 1 = (65536)^2 + 1 \equiv (154)^2 + 1 = 23717 \equiv 0 \pmod{641}$. (i) $2^{2^{n+1}} \equiv (-1)^2 \equiv 1 \pmod{p}$. As usual, putting $2^{n+1} = qe + r$ with $0 \leq r < e$ shows that $r = 0$. (ii) If $e|2^n$, then $-1 \equiv 2^{2^n} \equiv 1 \pmod{p}$ and so $p|2$. (iii) By (i) and (ii) $e = 2^{n+1}$. But $e|\phi(p) = p - 1$.